Building Success. Together.

Agenda Items

1. Cyber Incident Notification Regulations
2. Post COVID Landscape
   - Bank and Branch Impacts
   - Shift in Fraud Landscape
   - Potential Expansion of Reg E
3. ABA Resources

Cyber Incident Notification Regulations

- FFIEC Cyber Incident Notification Rule
- New Cyber Incident Reporting for Critical Infrastructure Act of 2022
- Proposed SEC rule on Notifications
- Proposed FTC Safeguards Rule: ‘Security Events’ Proposed Rule

FFIEC Cyber Incident Notification – Disruption Notice

- Computer Security Incident Notification Rule
  - "This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator…"
  - Compliance date May 1

- Disruption Notice – Banks
  - More than consumer data breach
  - Material operational disruption due to computer security failure
  - Notice to federal regulator within 36 hours – not full accounting but a "heads-up" by phone or email with short summary of situation

FFIEC Cyber Incident Notification

- 36-hour notice requirement:
  - Intent: Early warning of significant event
  - After “reasonable amount of time” for internal discussions to characterize incident
  - Incident will materially disrupt, degrade, or impair banking operations
  - Does not replace GLBA consumer data breach notice

- “Reasonable amount of time” to make a determination – NOT 36-hours after the incident occurs
  - Anticipates delay between:
  - (1) time when the incident occurs, and
  - (2) realization that an incident could severely disrupt, impair, or degrade banking operations

FFIEC Cyber Incident Notification

- Disruption Notice – Bank Service Providers
  - Once determined it has experienced computer-security incident has or is likely to materially disrupt for four or more hours
  - Bank service provider should notify bank customers as soon as possible
  - Bank determines if/when to escalate 3rd Party notice to bank supervisor

Cyber Incident Reporting for Critical Infrastructure Act

- CIRCIA mandates that DHS CISA develop and implement regulations requiring covered entities to report to CISA on covered cyber incidents and ransom payments within 72 hours
- Rulemaking will determine details
  - Covered entities those from Critical Infrastructure Sector
  - Covered cyber incidents undefined
  - What constitutes **"reasonable belief"** that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline
- CISA RFI due 11/12/2022 – Multiple trades engaging
- DHS nine regional listening sessions ongoing

Proposed SEC and FTC Notification Rules

- In May SEC Proposed Rule
  - Amend **Form 8-K** to require registrants to disclose information about a material cybersecurity incident within **four business days** after the registrant determines that it has experienced a material cybersecurity incident;

- FTC Safeguards Rule: 'Security Events' Proposed Rule
  - FTC's "security events" proposed rule would amend the Safeguards Rule to require "financial institutions" to report to the commission on security events that would impact at least 1,000 consumers.

  - The timing requirement would be "as soon as possible, and no later than 30 days after discovery of the event" (prominent Hill legislation, in comparison, would require a 72-hour reporting deadline

COVID – Impact on Banks

- As COVID spread in spring of 2020 dramatically impacted operations
  - Lockdowns impacted staff ability to travel
  - Branches closed
  - Remote work and remote assessments became the norm
- Several common practices implemented once lockdowns eased
  - Shift to drive through banking
  - Branch restrictions and “curbside banking”
  - Push for electronic banking options
  - Increased ATM use
  - Implementation of dividers, improved airflow and filtration

Staff Impacts

- Banks invested quickly to allow some level of remote work – required significant investments
  - VPN upgrades
  - Printer lockdown capabilities
  - Internal threat programs
- Ongoing impacts to staffing levels
  - Competition from local businesses
  - Inability to maintain staff levels to keep some branches open
- Regulators also moved to remote assessments
  - Generally positive response from bankers
  - Likely to continue some type of hybrid remote assessment program

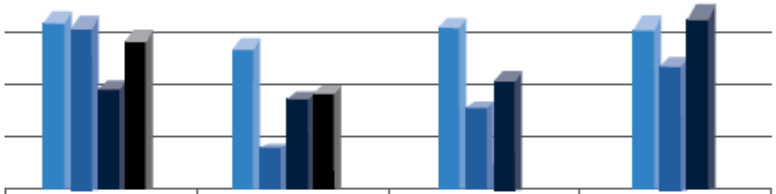
Impact on Branch Security and Operations

- Bank robberies down then bounced back – FBI Bank Crime Statistics
  - 2018 – 3033 Violations
  - 2019 – 2440
  - 2020 – 1788 – significant drop
  - 2021 – 1964 – increase but not to 2019 levels
- Robberies been trending downward but branches also closing*
  - 4000 branches closed since March 2020
  - Rate of 201 closings per month versus historical 10 year average of 99 per month
  - 9% of all branches closed since 2017

*https://ncrc.org/the-great-consolidation-of-banks-and-acceleration-of-branch-closures-across-america/

Bank Robbery Trends

Bank Robbery by Year & Quarter

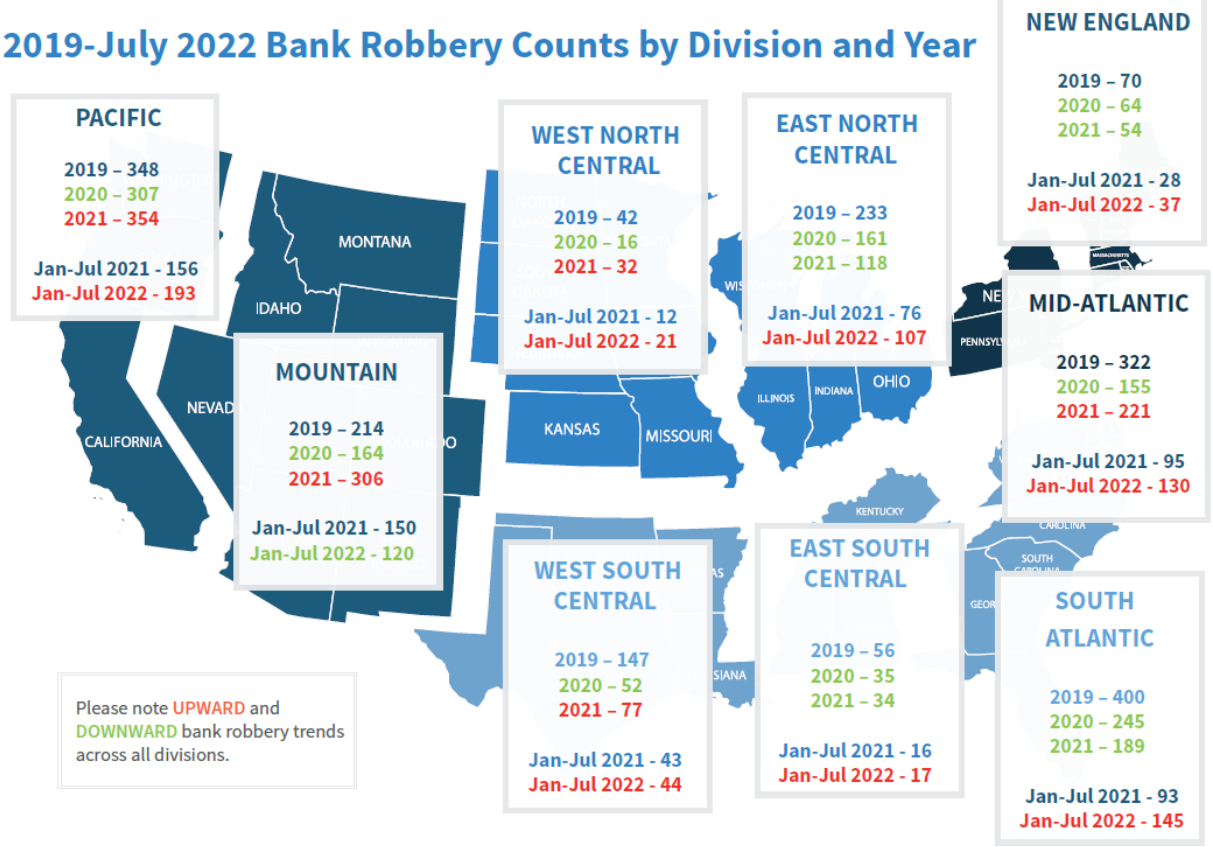


	Q1	Q2	Q3	Q4
2019	483	410	465	474
2020	475	124	237	363
2021	296	265	323	501
2022	436	281		

2019-2022 ABA Bank Capture Robbery Analysis

Key Observations

- Bank robbery counts show significant variation during the 2019-2021 time period, which can be attributed to COVID-19 restrictions, policy modifications, and closings.
- The Q4 2021 counts surpass the number of robberies for the same quarter in the two preceding years as well as all of the other individual quarters during the study period.
- There was a 34.6% decrease in bank robberies for the full year of 2020 vs. 2019 and a 15.5% increase for the full year of 2021 vs. 2020.
- The most recent months suggest that bank robbery counts may be returning to pre-COVID levels. However, it should be noted that the magnitude of this trend varies by bank.



2019-2022 ABA Bank Capture Robbery Analysis

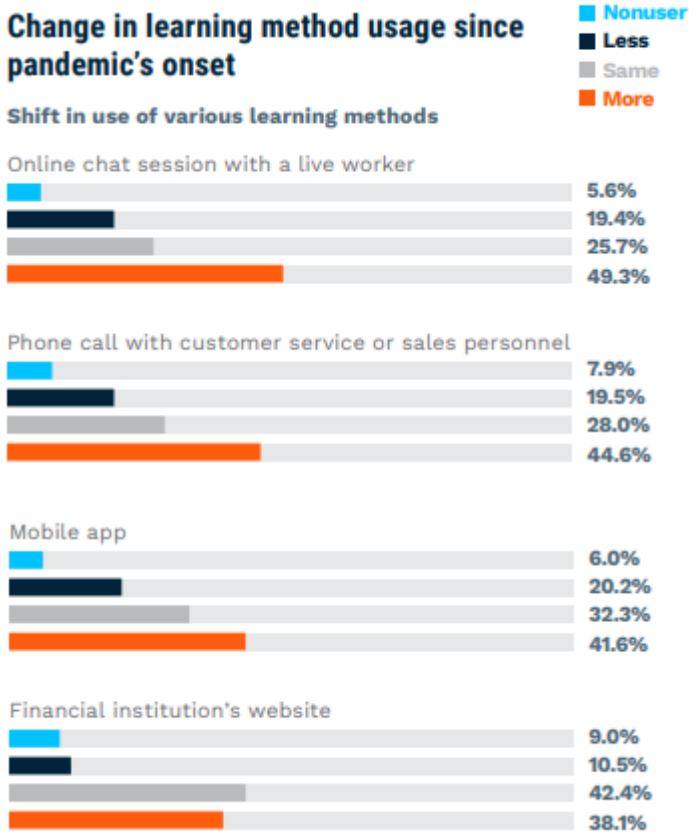
Assault Trendlines

2019	151		6,411		3,486		1,214	
2020	135	-10.6%	5,836	-9.0%	2,229	-36.1%	934	-23.1%
2021	154	14.1%	5,584	-4.3%	2,540	14.0%	1,126	20.6%
Jan 2021 - June 2021	71		2,601		1,142		551	
Jan 2022 - June 2022	82	15.5%	3,063	17.8%	1,476	29.2%	595	8.0%

CAP Index Report for August ABA Bank Security Committee Meeting

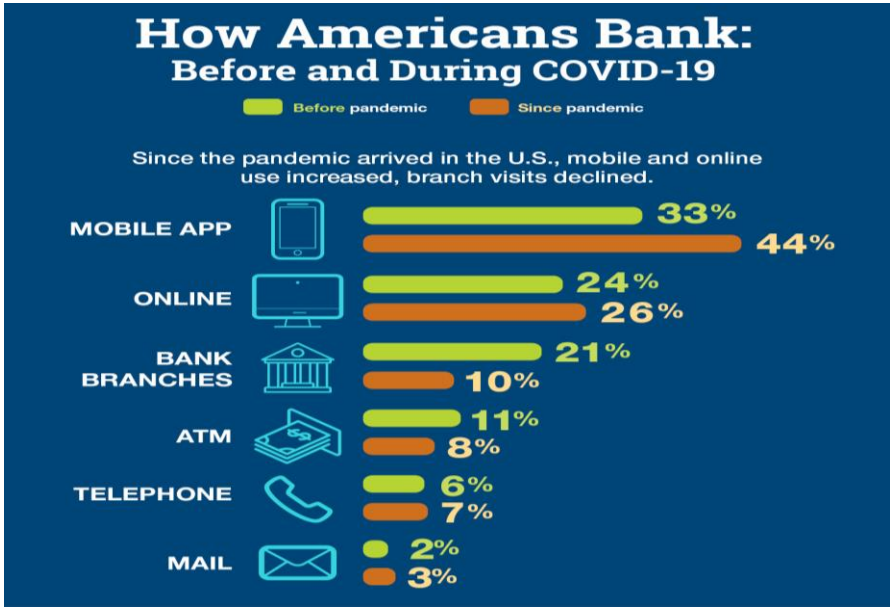
Shift to Digital

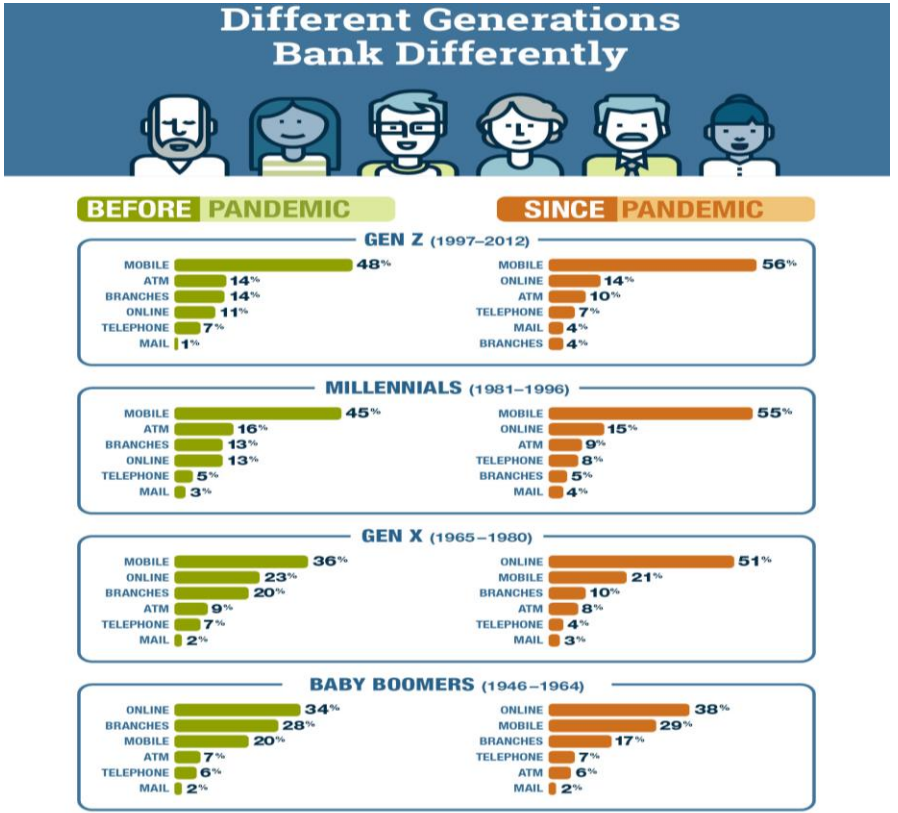
- Consumers were already moving to digital access but COVID accelerated shift
- Chase Digital Banking Survey 2021
  - Four in five customers prefer to manage their finances digitally rather than in person.
  - Roughly eight in 10 use a smartphone and/or desktop/laptop to complete banking activities.
  - The vast majority of Chase (89%) and non-Chase (85%) customers feel they save time by managing their finances digitally.



PYMNTS: Retail Banking Services Paradigm Shift

Shift to Digital





ABA Sponsored Morning consult poll Oct 2021

Potential Shift in Focus at Branches

- Adoption of digital technologies, mobile apps and peer to peer payment applications have reduced need for branch visits
- Likely branch operations may shift to focus on important life moments
  - Buying a home or vehicle
  - Estate planning
  - College tuition
- Move from daily transactions to a focus on more personalized service
  - Creation of more private spaces for longer discussions
  - More of welcoming environment – lounge type setting
  - Some banks already adopting this type of model

COVID – Impact on Fraud

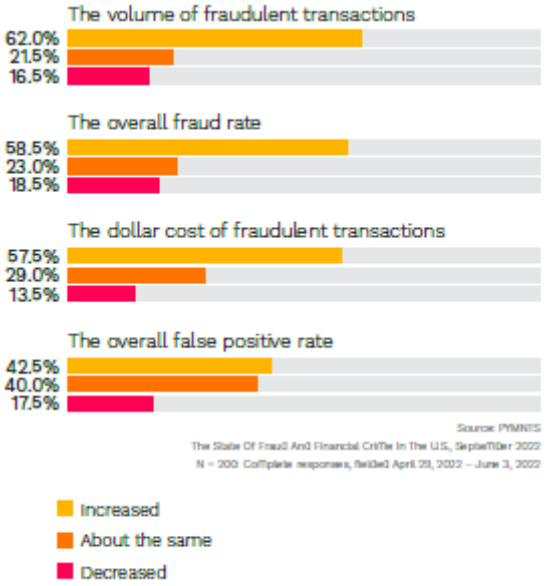
- During pandemic fraudsters shifted to PPP, EIDL and unemployment insurance
- PPP loans
  - Some estimates put PPP loan fraud at $76B, nearly 10% of total programmatic budget of $800B
  - Fintech lenders made 29% of loans but accounted for more than half of suspicious loans
  - Last week DoJ announced first settlement with bank that improperly processed PPP loan
  - Recent law extended statue of limitations to 10 years
- Unemployment insurance fraud

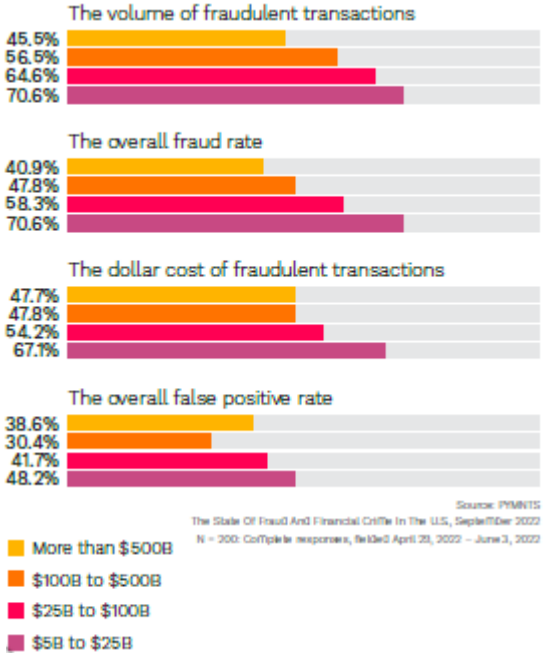
COVID – Impact on Fraud

- Unemployment insurance fraud may actually dwarf amount of PPP fraud
- State workforce agencies were woefully unprepared for unemployment insurance
  - ABA worked closely with National Association of State Workforce Agencies
  - No account validation procedures
  - No fundamental checks on identity or work history
- Estimates put amount of fraud in $100's of billions
  - Claims from March to December 2020 equated to 68% of US workforce even though unemployment was 23%
  - Five states AZ, GA, HI, NV, RI claims outnumbered pool of workers
  - Individual states estimate fraud from 10% to 90% of claims

Post COVID – Shift Back to Cyber-enabled Fraud

- Fraudsters shift back to traditional fraud opportunities
  - Ransomware
  - P2P payment frauds
  - Check fraud
- PYMNTS Survey
  - 59% FIs experienced increased fraud
  - 77% of firms had losses between $2.5 - $5M

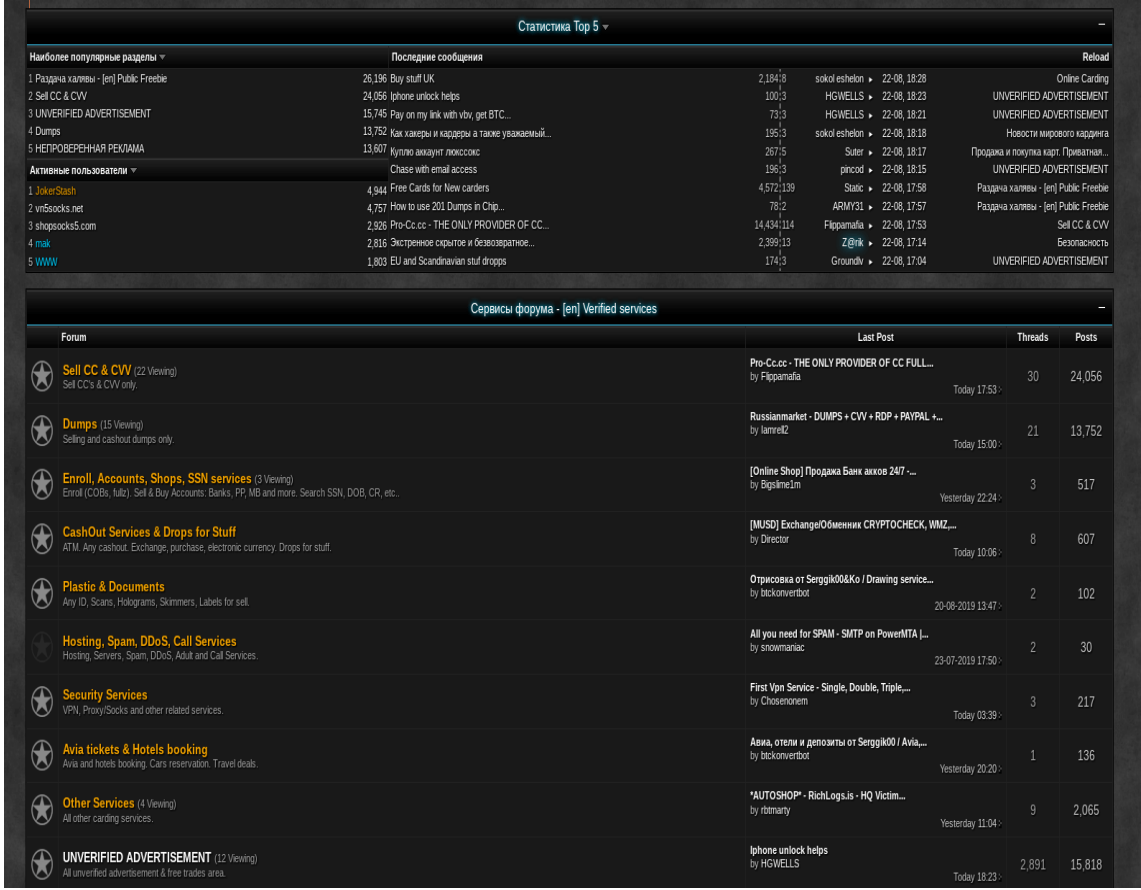




Dark Markets

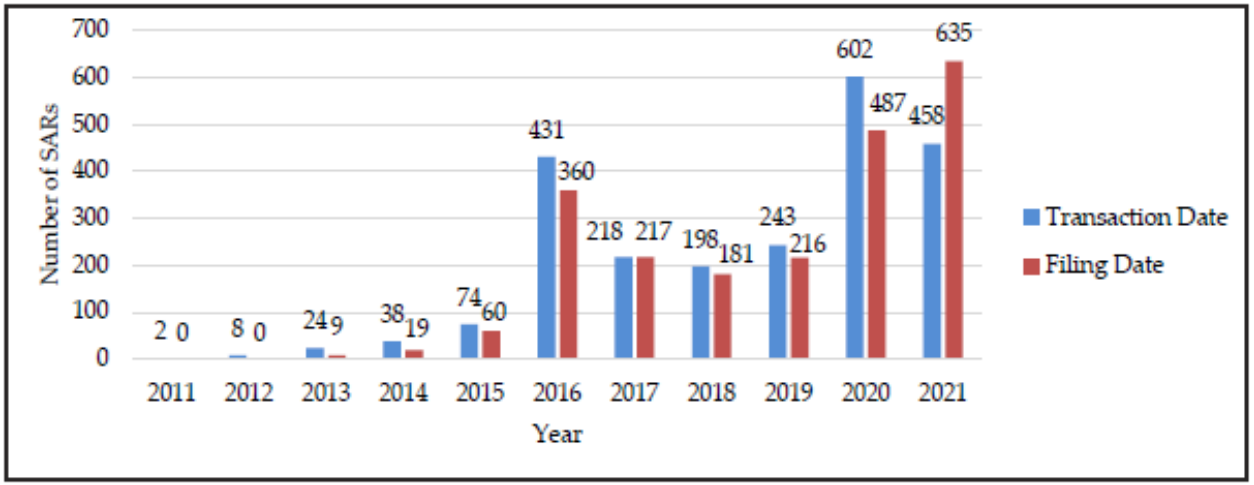
Anonymous interaction using TOR

- Phishing kits
- Ransomware as service
- “Credit Card number sells for $2 on the black market while a health record goes for $20 or more…”
  -Peter B. Nichol, PMP, CSSMBB
- “Social Security Number sells for $1.00 and a drivers license $20…”
  -FiVerity
- Cashout/Mule Services

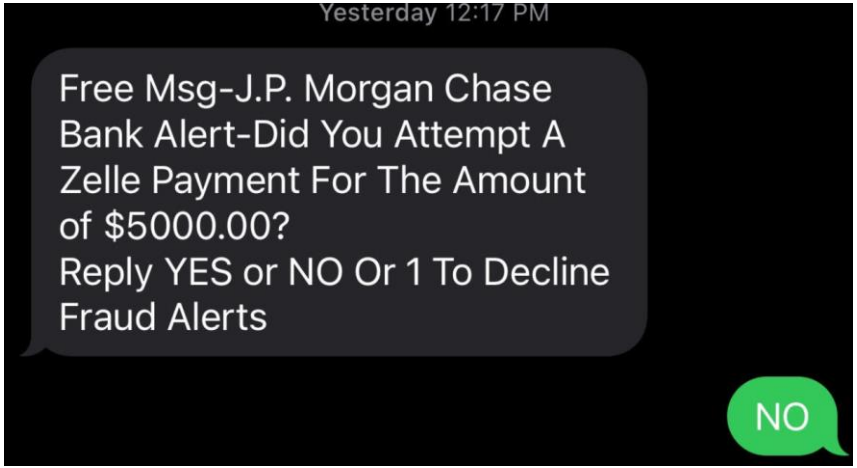


Ransomware - FinCEN Financial Trend Analysis

- First six months 2021 - 30% increase in ransomware SARs over all of 2020
- 2021 SAR values will exceed previous 10 years combined
- Potential ransomware payments to 177 Bitcoin wallets - **$5.2B transactions**



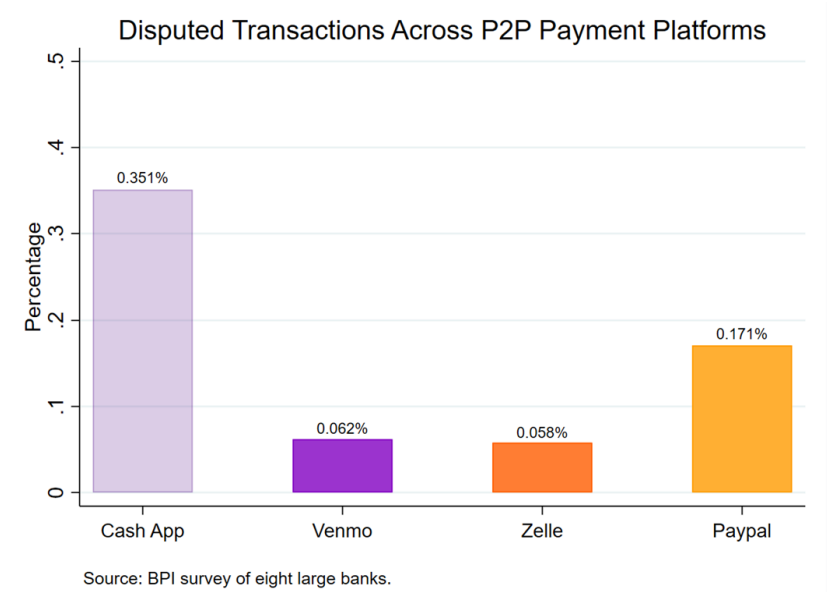
P2P Fraud



- After victim responds (yes or no), fraudster calls them
- Fraudster socializes username and initiates password change
  - To defeat 2 step auth, fraudster keeps victim on phone and gets passcode to change password
- Password is changed and P2P payments are made to fraudsters accounts

P2P Payment Complaints

- See CFPB complaint database
  Zelle had the fewest complaints
- Out of 2,944,468 total complaints
  - Paypal" had 11,990 matches
  - "venmo" 681 matches
  - "cashapp" 609 matches
  - "zelle" 509 matches



Reg E Expansion Challenges

- Wall Street Journal article discussed plans by CFPB to expand Reg E coverage to authorized transactions that are “fraudulently induced”
- ABA believes this is illegal expansion of authority and along with other trades strongly pushing back
- CFPB hosting meeting this Thursday (29th) with trades and their members
  - “to hear your assessment of challenges faced by consumers with respect to fraudulent peer-to-peer (P2P) transactions.”
  - Multiple trades attending (ABA, ICBA, BPI, CUNA, etc.)
  - Each trade only allowed to bring two banker reps – ABA bringing $150M and $1.5B bank

Additional Efforts to Push Regulators to Action

- FCC issued Seventh Notice of Proposed Rulemaking on implementation of improved CallerID rules - STIR/SHAKEN framework
  - ABA submitted comment asking them to end waivers and not allow displaying of data without highest level of authentication
- The Federal Trade Commission has proposed a rule to fight government and business impersonation scams
  - ABA focusing comment efforts on ensuring CallerID impersonation is included
- Pushing DoJ to provide law enforcement resources to investigate

Back to the Basics – Check Fraud

Problem

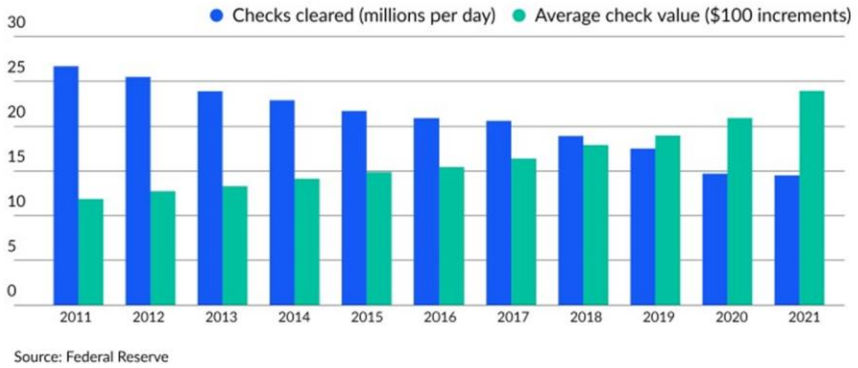
- Per Catalyst Corporate, who represents 1,400 Federal Credit Unions, Check fraud accounted for **66% of payment fraud**, followed by 39% for wire transfers in 2021

Challenges

- Creating backlogs in check warranty claims
- Availability of funds (Rec CC & Check 21)
- Average check value doubled last decade

FinCEN SAR Statistics

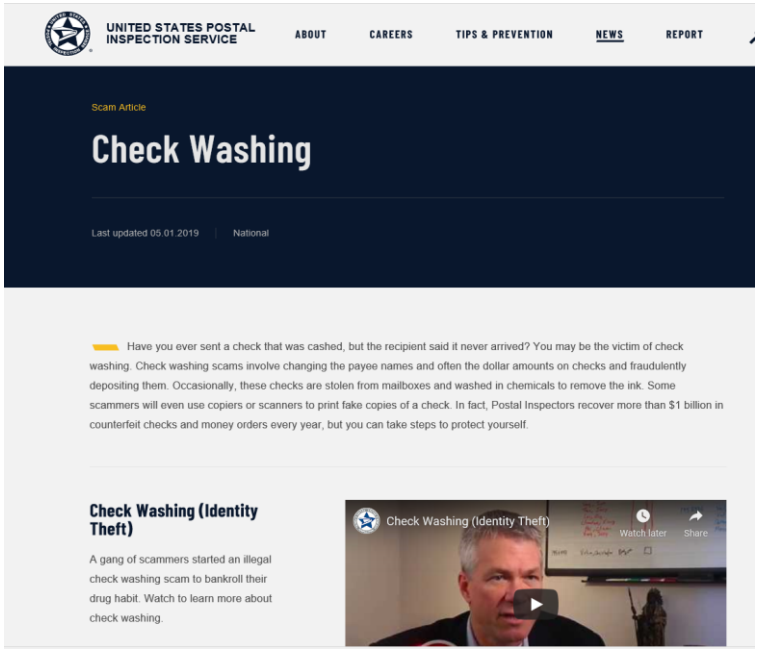
Suspicious Activity Category	Suspicious Activity Type	2014	2020	2021
Fraud	ACH	24,904	143,269	176,911
	Check	96,786	216,963	249,802
	Credit/Debit card	75,496	132,925	140,327



Source: Federal Reserve

What's Happening on the Street

Theft of Arrow Key



Resources Available to Help

- ABA BanksNeverAskThat Campaign
- ABA Fraud Information Sharing Exchange (AFix)
- ABA Ransomware Toolkit
- Additional Government Resources

#BanksNeverAskThat Campaign

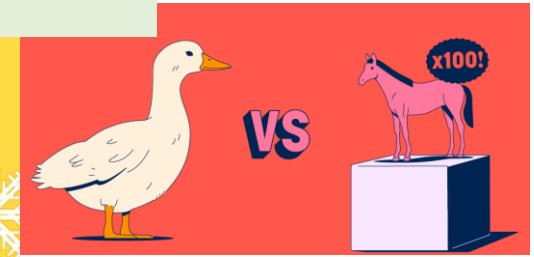
Goal:

Build on the success of the past two years by refreshing the website and creating new assets that reflect the current landscape around scams, including Mobile Payment Apps.

#BanksNeverAskThat Campaign

Theme:

Use humorous videos, social posts, digital signage and more to highlight questions banks would never ask their customers.



BANKS NEVER ASK THAT

Campaign Results to Date:

- **2,043 banks** in all 50 states
- More than **600,000 visits** to website
- **94,000** tested their skills
- **175,000** video views

American Bankers Association

ABA 314b Fraud Information Exchange (AFix)

Intelligence sharing network to enhance banks' ability to identify and defend against fraudulent transactions

Aggregates & centralizes suspect account information associated with potential bad actors and/or fraudulent accounts, allowing participants to proactively identify and act against future transactions

Aligns to FinCEN's expectation that financial institutions share data to identify and report on activities associated with fraud, money laundering and terrorist financing

See FinCEN's Section 314(b) Fact Sheet (Dec. 2020)

Offers participants **safe harbor protections**

AFix Pilot Program

- ABA received FinCEN approval as a 314(b)-sharing entity and will parent the exchange forum and platform
- Created a 314(b) Sharing Advisory Group
- Working with JPMC Onyx customizing a blockchain network, LiiNK, to host a secure, exclusive 314b exchange platform
  - Both API & UI (easy queries) system access will be deployed
  - Use cases include recording Probable Fraud and Possible Fraud
  - Go live first quarter 2023

Resources

- ABA Ransomware Toolkit released last week
- Toolkit has succinct one-page guides
  - How to Respond to a Ransomware Attack
  - Ransomware: Should You Pay Up? It Depends
  - Protect Your Bank Against Ransomware
- Find the toolkit at https://aba.com/ransomware

Additional Resources

- CISA has several resources:
  https://cisa.gov/cybersecurity
  https://cisa.gov/stopransomware

- USSS Preparing for a Cyber Incident includes several resources:
  https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

- FBI IC3:
  https://www.ic3.gov/

- Federal Reserve Bank Synthetic ID Toolkit
  https://fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/synthetic-identity-fraud-basics/

QUESTIONS

Paul Benda
pbenda@aba.com